

CES-35

Lab1 - Wireshark

# Objetivo

Observar a sequência de trocas de mensagens entre duas entidades, investigando os detalhes da operação dos protocolos.

Você executará vários aplicativos de rede em diferentes cenários usando seu computador. Você observará os protocolos de rede em seu computador "em ação", interagindo e trocando mensagens com entidades de protocolo em execução em outro lugar na Internet.

# Sniffers

Farefajor de pacotes (sniffer): ferramenta básica para observar as mensagens trocadas entre entidades de protocolo em execução.

Um sniffer copia passivamente ("fareja") as mensagens enviadas e recebidas pelo computador; ele também exibirá o conteúdo dos vários campos de protocolo dessas mensagens capturadas.

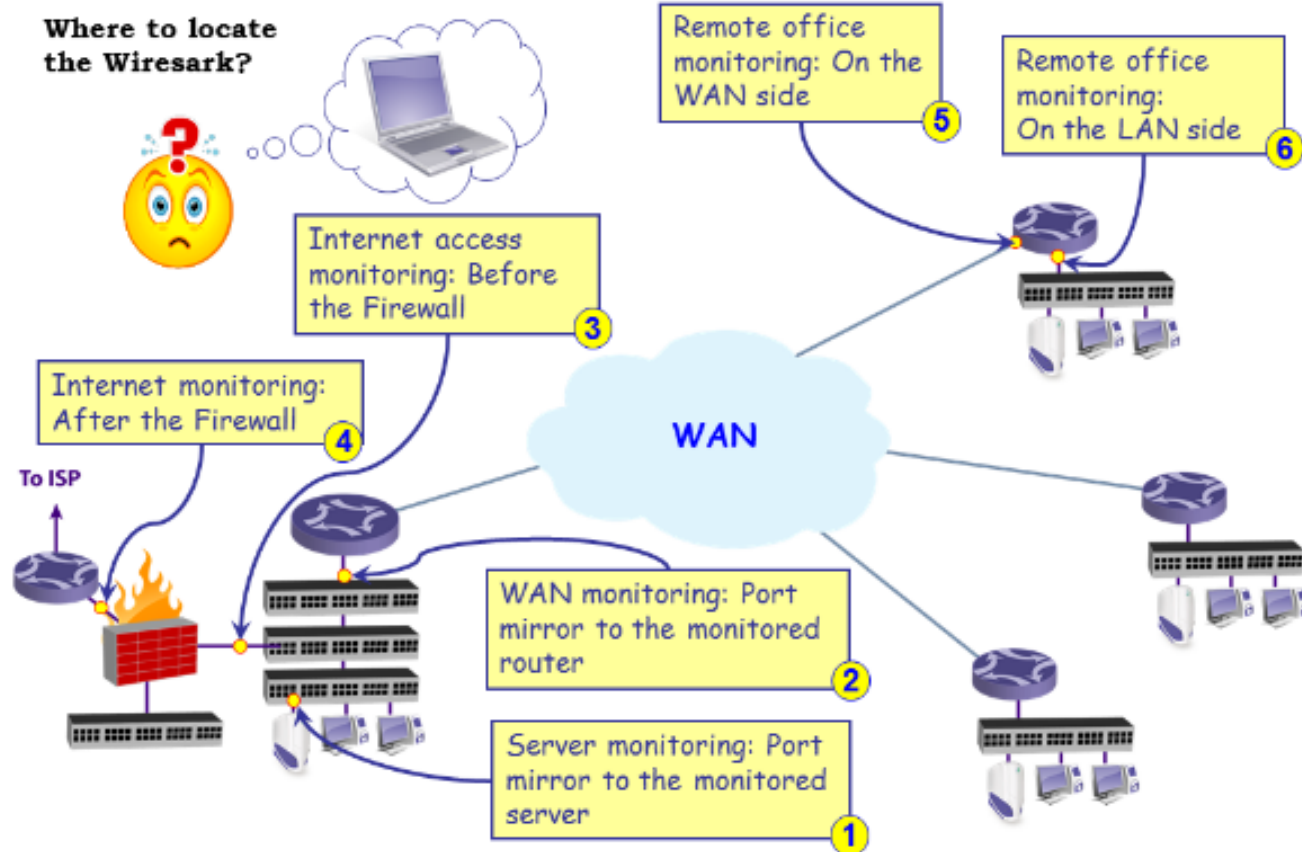
Para esses laboratórios, usaremos o farejador de pacotes

**Wireshark** um farejador de pacotes gratuito / shareware que roda em computadores Windows, Linux / Unix e Mac

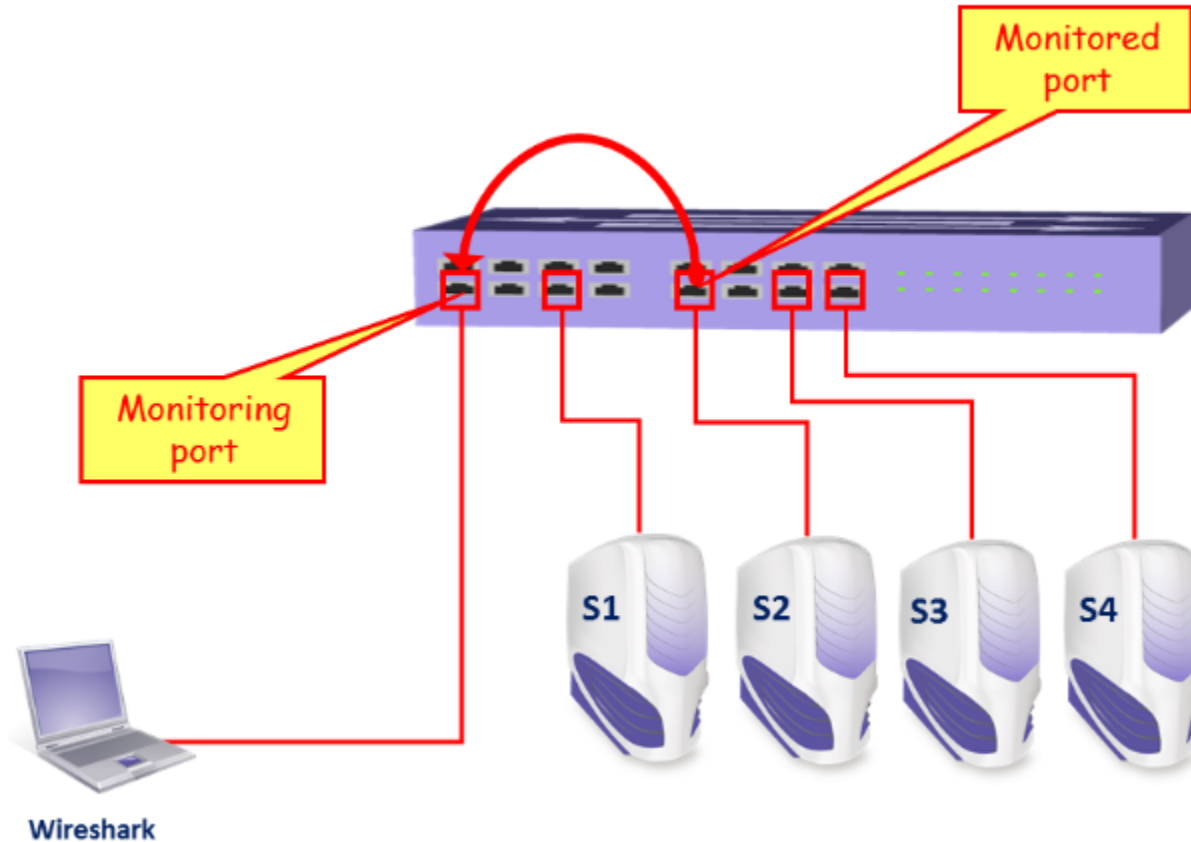
# Para que serve?

- Compreender o funcionamento normal/anormal;
- Descobrir problemas da rede;
- Obter estatísticas da rede;
- Ensino;

# Onde posicionar Sniffers?



# Espelhando uma porta



# Algumas perguntas

## Does Wireshark affect network performance?

No. Wireshark is a listener, it doesn't generate traffic. However, if you set a switch on the system to duplicate all passing traffic to send to the Wireshark-monitored port then network traffic will be increased and performance could be impaired.

## Is it illegal to use Wireshark on a public wifi?

It is not illegal to use Wireshark anywhere, however, there are some illegal activities that can be facilitated by Wireshark. Think of Wireshark as being like a telescope. It is not illegal to look through the air with a telescope at passing cars, but it is illegal to use it to look through someone's window.

# Limites

## ★ What we can:

- Capture packets
- Watch smart statistics
- Define filters – capture and display
- Analyze problems

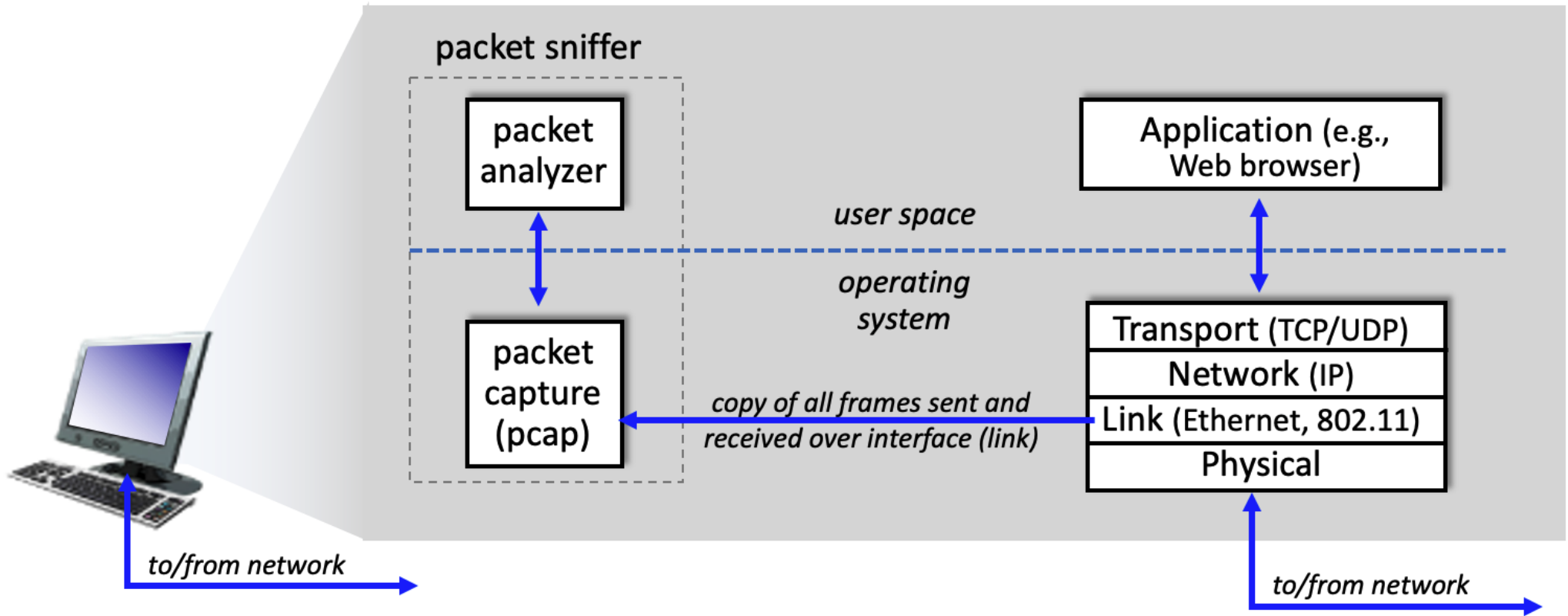
## ★ What we cannot:

- It is not an automatic tool
- It is not suitable for long-term monitoring
- It is not a “magic” tool

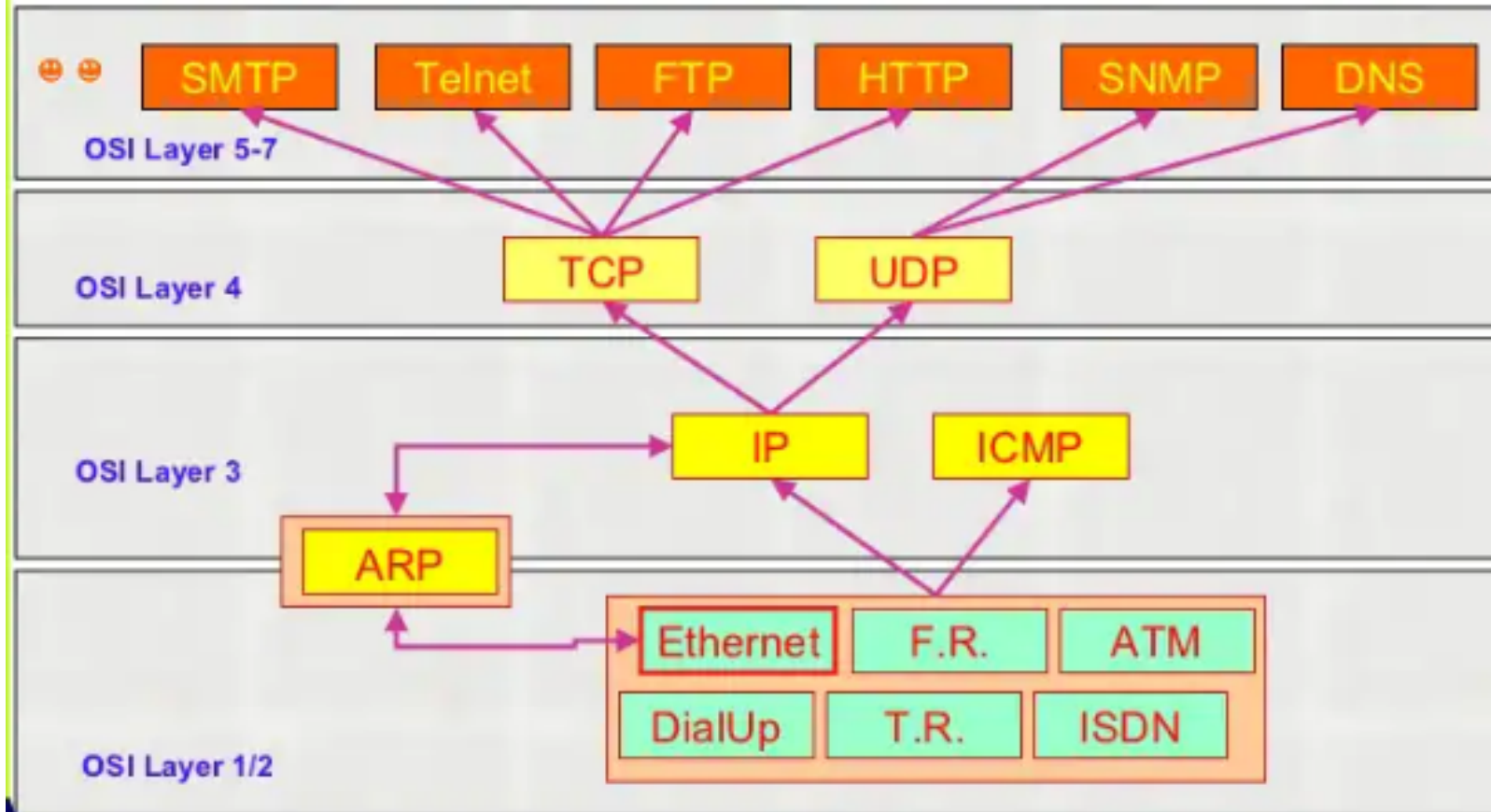




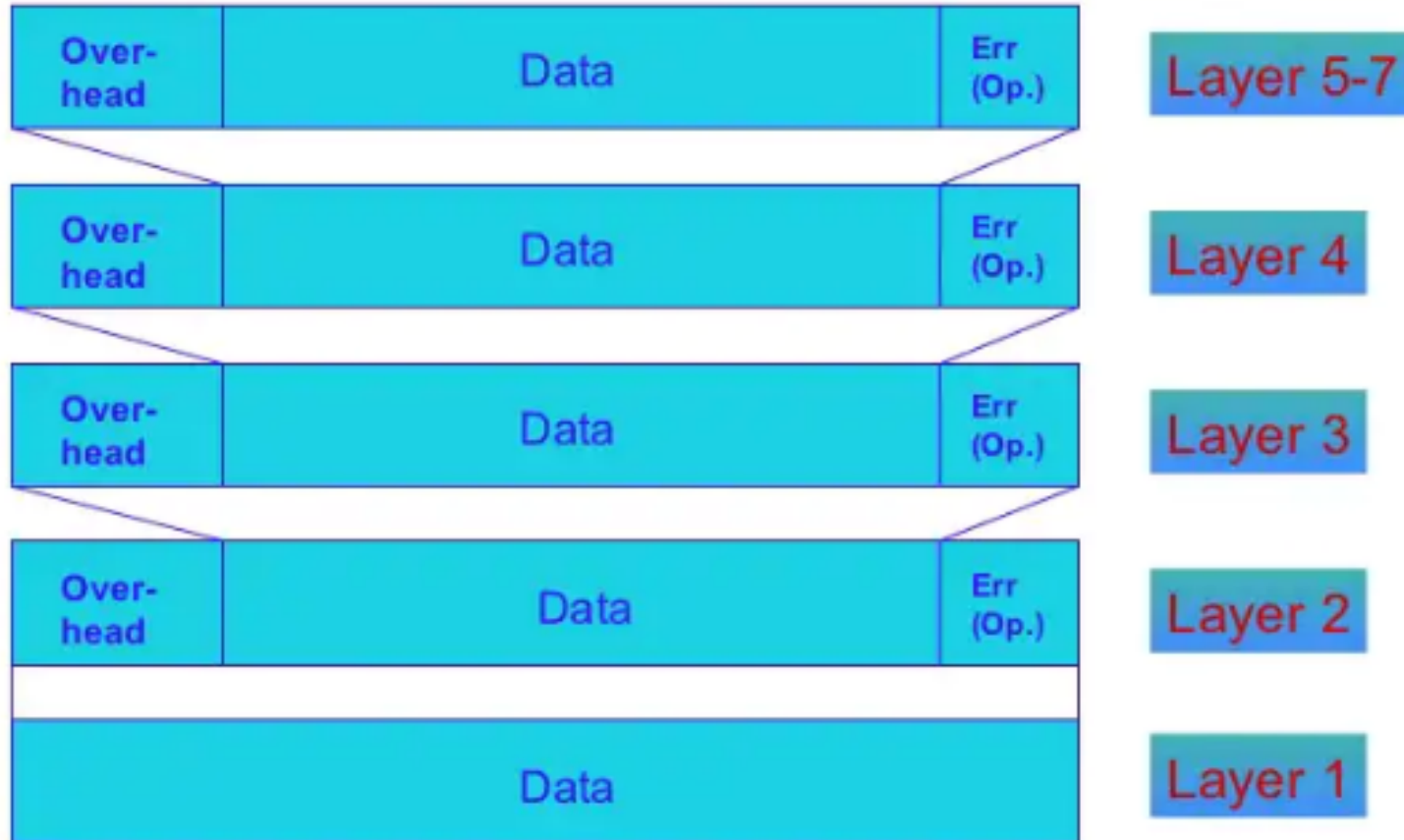
# Estrutura de um sniffer



# Lembrando das camadas...

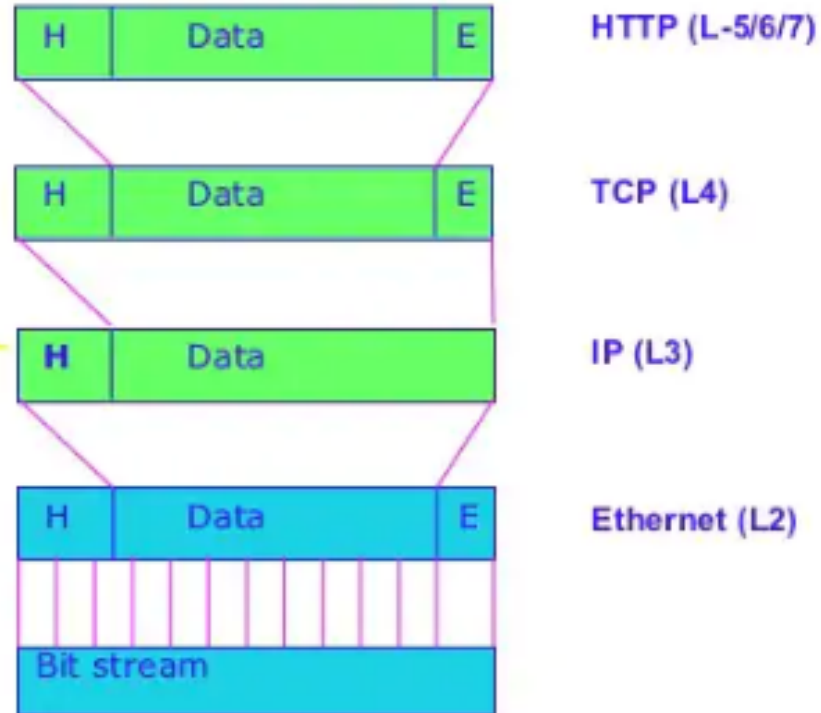


# Estrutura de dados

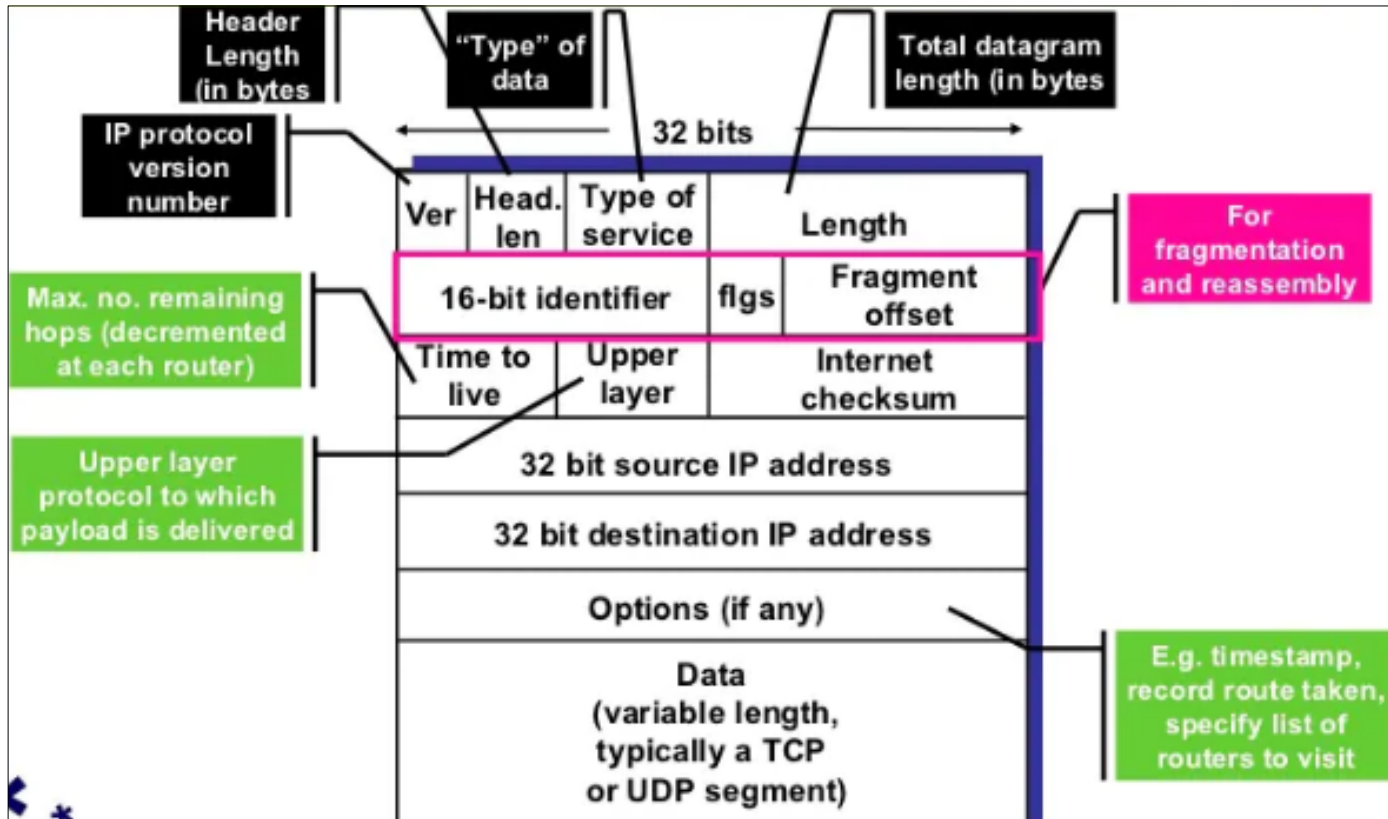


# Exemplo – Camada 3

This is the IP header

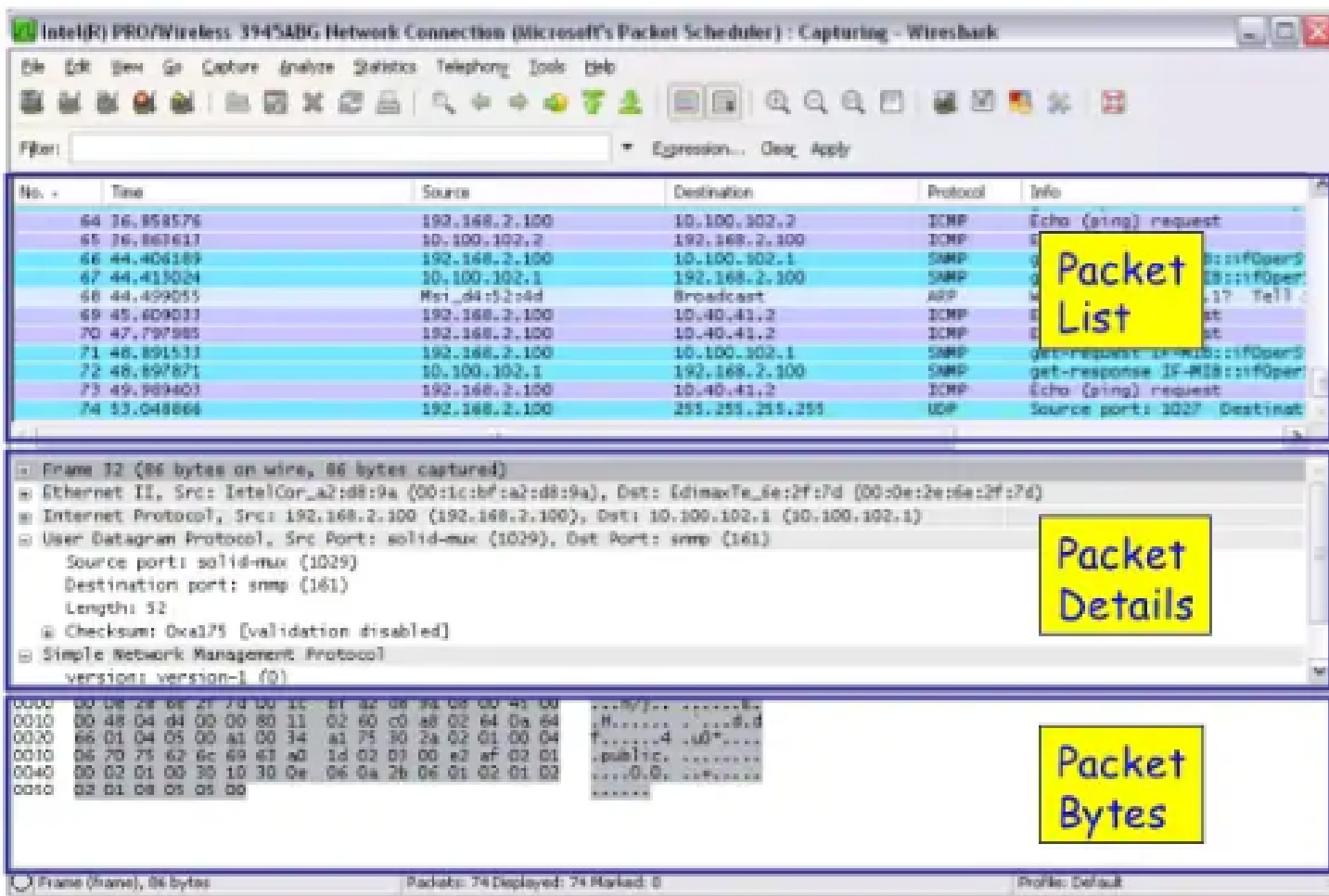


# Exemplo – Cabeçalho IP



```
struct iphdr {  
#if defined(__LITTLE_ENDIAN_BITFIELD)  
    __u8    ihl:4,  
            version:4;  
#elif defined (__BIG_ENDIAN_BITFIELD)  
    __u8    version:4,  
            ihl:4;  
#else  
#error "Please fix <asm/byteorder.h>"  
#endif  
  
    __u8    tos;  
    __be16  tot_len;  
    __be16  id;  
    __be16  frag_off;  
    __u8    ttl;  
    __u8    protocol;  
    __sum16 check;  
    __be32  saddr;  
    __be32  daddr;  
    /*The options start here. */  
};
```

# Wireshark capturando



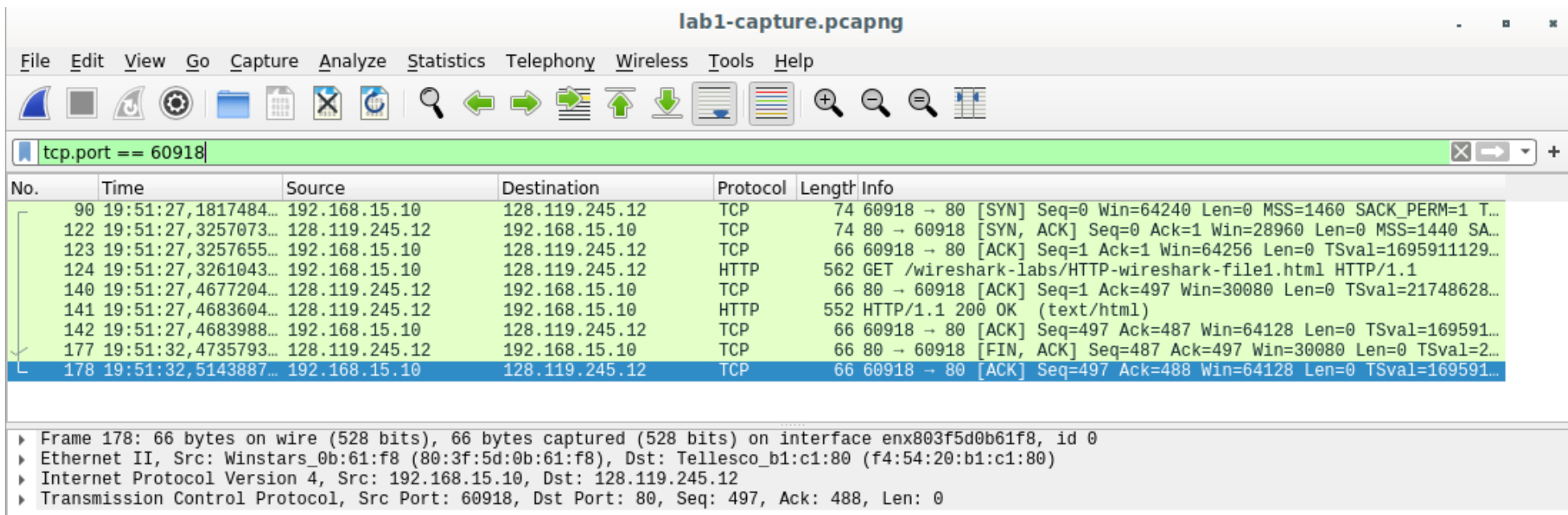
# Wireshark – Packet list

## Columnas:

- No - Represents a specific sequence number of the network packet. To classify a given packet, one can use this.
- Time - This is the time that a specific packet has been recorded.
- Source - This represents where we are getting the packets from. This is denoted as Internet Protocols (IP Addresses).
- Destination - This is used to represent the Internet Protocol(IP Address) where the packet is going.
- Protocol - This refers to the protocol of the data you have captured. This could be TCP, ARP etcetera
- Length- This is used to represent the size of the packet captured.
- Info - Additional information about the packet you have captured.

# Wireshark – Filter

Existe uma sintaxe própria para filtrar os pacotes:



The screenshot shows the Wireshark interface with the title bar "lab1-capture.pcapng". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and packet analysis. The filter bar at the top displays the active filter: `tcp.port == 60918`. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 178 is selected and highlighted in blue. Below the packet list, the packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
90	19:51:27,1817484...	192.168.15.10	128.119.245.12	TCP	74	60918 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
122	19:51:27,3257073...	128.119.245.12	192.168.15.10	TCP	74	80 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SA...
123	19:51:27,3257655...	192.168.15.10	128.119.245.12	TCP	66	60918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1695911129...
124	19:51:27,3261043...	192.168.15.10	128.119.245.12	HTTP	562	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
140	19:51:27,4677204...	128.119.245.12	192.168.15.10	TCP	66	80 → 60918 [ACK] Seq=1 Ack=497 Win=30080 Len=0 TSval=21748628...
141	19:51:27,4683604...	128.119.245.12	192.168.15.10	HTTP	552	HTTP/1.1 200 OK (text/html)
142	19:51:27,4683988...	192.168.15.10	128.119.245.12	TCP	66	60918 → 80 [ACK] Seq=497 Ack=487 Win=64128 Len=0 TSval=169591...
177	19:51:32,4735793...	128.119.245.12	192.168.15.10	TCP	66	80 → 60918 [FIN, ACK] Seq=487 Ack=497 Win=30080 Len=0 TSval=2...
178	19:51:32,5143887...	192.168.15.10	128.119.245.12	TCP	66	60918 → 80 [ACK] Seq=497 Ack=488 Win=64128 Len=0 TSval=169591...

Frame 178: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface enx803f5d0b61f8, id 0  
Ethernet II, Src: Winstars\_0b:61:f8 (80:3f:5d:0b:61:f8), Dst: Tellesco\_b1:c1:80 (f4:54:20:b1:c1:80)  
Internet Protocol Version 4, Src: 192.168.15.10, Dst: 128.119.245.12  
Transmission Control Protocol, Src Port: 60918, Dst Port: 80, Seq: 497, Ack: 488, Len: 0

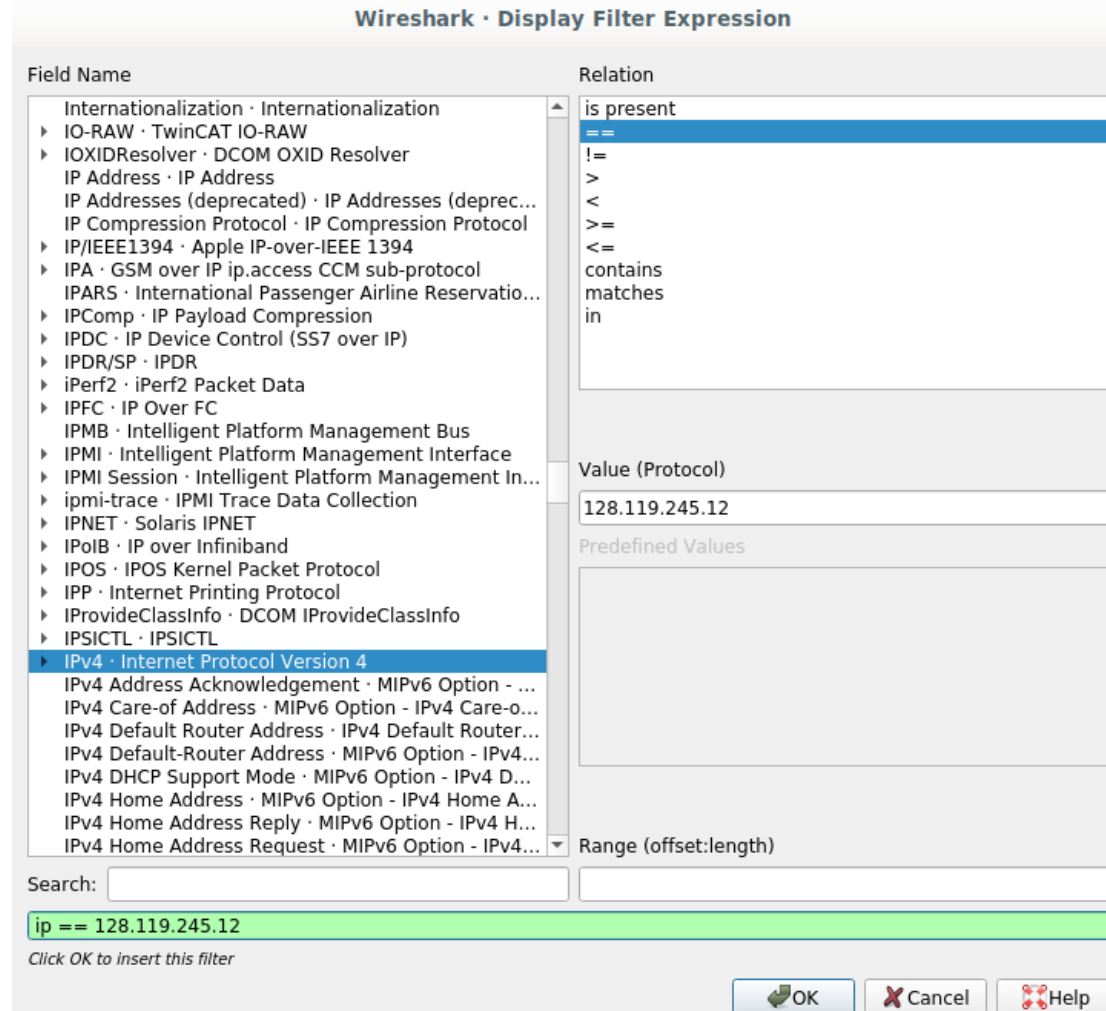


# Wireshark – como construir o filtro

Analyze → Display Filter Expression  
→ ipv4.

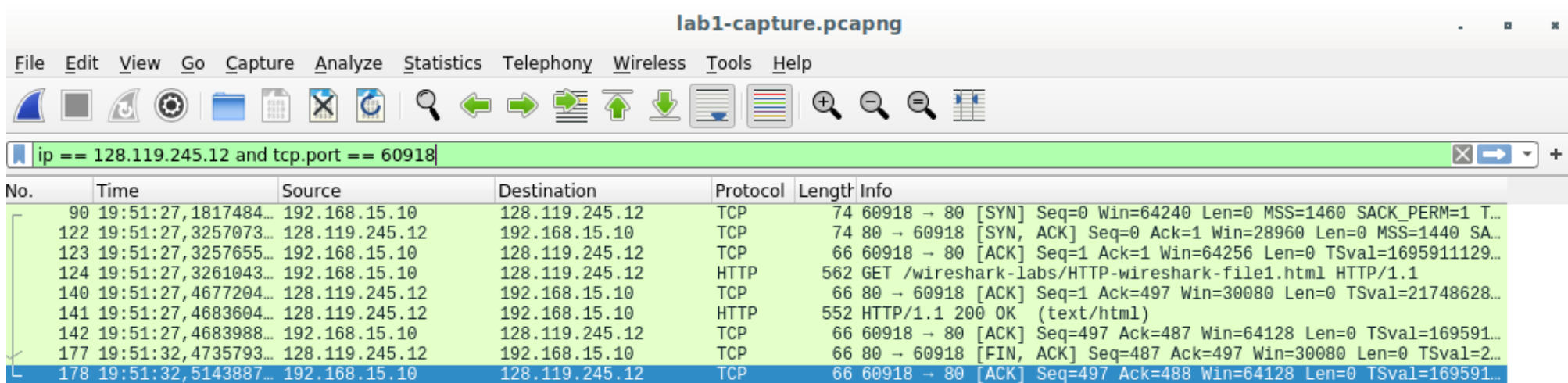
Escolha a opção de seu interesse, no  
meu caso o endereço do site do  
Kurose.

É possível compor condições para  
formar filtros mais completos e  
específicos.



# Wireshark – como construir o filtro

Filtro que seleciona IP e porta dos pacotes envolvidos com a transferência da página.



The screenshot shows the Wireshark interface with the file 'lab1-capture.pcapng' open. The packet capture filter is set to 'ip == 128.119.245.12 and tcp.port == 60918'. The packet list shows 18 packets, with the last packet (No. 178) selected. The packet details pane shows the selected packet's structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
90	19:51:27,1817484...	192.168.15.10	128.119.245.12	TCP	74	60918 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
122	19:51:27,3257073...	128.119.245.12	192.168.15.10	TCP	74	80 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SA...
123	19:51:27,3257655...	192.168.15.10	128.119.245.12	TCP	66	60918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1695911129...
124	19:51:27,3261043...	192.168.15.10	128.119.245.12	HTTP	562	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
140	19:51:27,4677204...	128.119.245.12	192.168.15.10	TCP	66	80 → 60918 [ACK] Seq=1 Ack=497 Win=30080 Len=0 TSval=21748628...
141	19:51:27,4683604...	128.119.245.12	192.168.15.10	HTTP	552	HTTP/1.1 200 OK (text/html)
142	19:51:27,4683988...	192.168.15.10	128.119.245.12	TCP	66	60918 → 80 [ACK] Seq=497 Ack=487 Win=64128 Len=0 TSval=169591...
177	19:51:32,4735793...	128.119.245.12	192.168.15.10	TCP	66	80 → 60918 [FIN, ACK] Seq=487 Ack=497 Win=30080 Len=0 TSval=2...
178	19:51:32,5143887...	192.168.15.10	128.119.245.12	TCP	66	60918 → 80 [ACK] Seq=497 Ack=488 Win=64128 Len=0 TSval=169591...

# Wireshark FlowGraph

Em Statistics →  
FlowGraph clique  
em  
Limit to display  
filter,  
E verá os pacotes  
do fluxo  
selecionado no  
filtro.

Wireshark · Flow · lab1-capture.pcapng

Time	192.168.15.10	128.119.245.12	Comment
8.185767258	60918	60918 → 80 [SYN] Seq=0 Win=64240 Len=0	TCP: 60918 → 80 [SYN] Seq=0 Win=64240 Len=0 ...
8.329726221	60918	80 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=...	TCP: 80 → 60918 [SYN, ACK] Seq=0 Ack=1 Win=2...
8.329784360	60918	60918 → 80 [ACK] Seq=1 Ack=1 Win=64256	TCP: 60918 → 80 [ACK] Seq=1 Ack=1 Win=64256 ...
8.330123172	60918	GET /wireshark-labs/HTTP-wireshark-file1.ht	HTTP: GET /wireshark-labs/HTTP-wireshark-file1.ht...
8.471739252	60918	80 → 60918 [ACK] Seq=1 Ack=497 Win=3000	TCP: 80 → 60918 [ACK] Seq=1 Ack=497 Win=300...
8.472379274	60918	HTTP/1.1 200 OK (text/html)	HTTP: HTTP/1.1 200 OK (text/html)
8.472417690	60918	60918 → 80 [ACK] Seq=497 Ack=487 Win=...	TCP: 60918 → 80 [ACK] Seq=497 Ack=487 Win=6...
13.477598178	60918	80 → 60918 [FIN, ACK] Seq=487 Ack=497 W...	TCP: 80 → 60918 [FIN, ACK] Seq=487 Ack=497 Wi...
13.518407586	60918	60918 → 80 [ACK] Seq=497 Ack=488 Win=...	TCP: 60918 → 80 [ACK] Seq=497 Ack=488 Win=6...

Packet 123: TCP: 60918 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1695911129 TSecr=2174862745

☒ Limit to display filter

Flow type: All Flows

Addresses: Any

Save As... Reset Diagram Close Help

# Instalando o Wireshark

No site [www.wireshark.org](http://www.wireshark.org) pode se fazer o download.

No Linux pode se instalar o pacote via comandos:

```
$sudo apt update
```

```
$sudo apt-get install wireshark
```

```
$sudo wireshark
```

Siga o roteiro e responda as perguntas.